DEPARTMENT OF THE ARMY
15TH REGIMENTALSIGNAL BRIGADE
FORT GORDON, GEORGIA 30905-5729

REPLY TO
ATTENTION
OF:

ATZH-TB 1 June 2011

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Policy Letter 20: Use of Automated Information Systems (AIS)

1. **References:**

   a. AR 25-1, Army Knowledge Management and Information Technology (4 Dec 2008)

   b. AR 380-5, Department of the Army Information Security Program (29 Sep 00)

   c. AR 25-2, Information Assurance (23 March 2009)

   d. Memo, IA BBP, 06-EC-O-0008: Data at Rest (DAR) Protection (18 Oct 06)

2. **Purpose:**

In December of 1987, Congress passed the Computer Security Act which became Public Law 100-23-5 in January of 1988. This law set forth a statutory requirement that all users, managers, supervisors, and commanders of Automated Information Systems (AIS) receive initial and annual training in automation security. The information contained in this memorandum fulfills the user-training requirement of both PL 100-23-5 and AR 25-2.

3. **Scope:**

Users will read this policy letter along with the attached SOP and complete IA Awareness Training to include providing security clearance documentation and acknowledgement of the policy guidance by signing an Acceptable User Policy statement (Enclosure 1) prior to receiving a Fort Gordon email and network access account. All personnel are required to review this policy and update their acceptable user policy statements annually. Supervisors will brief all personnel under their authority on this policy.

4. **Information Assurance Support Officer (IASO) Responsibility:**

The IASO is responsible for setting standards, enforcing prescribed policies, and individual user security training.

5. **Personal Responsibility:**

a. AIS users, supervisors, managers and commanders are required by regulations to apply prescribed security policies and procedures. Failure to do so may result in disciplinary action and penalties. Information systems security policies and procedures are found in Army regulations, USASC&FG supplements, SOPs and this document.

b. Before operating AIS, users must understand and comply with the security requirements of the system. Consult with an IASO if you have any questions on this policy.

c. Users must comply with the following automation security policies and procedures, which are divided into four areas: procedural security, data security, physical security and COMSEC. These policies and procedures are not all-inclusive; however, they constitute the minimum "do's and don'ts" of system operation.

d. Users are responsible for rebooting their AIS daily, locking their workstations upon leaving, and ensuring the screen locks on their workstations after 10 minutes of inactivity.

e. Safeguard user passwords and Personal Identification Number (PIN). Users will not reveal passwords or PIN to anyone nor store them in plain text on an AIS. Users are responsible for all activities occurring on the network under their logon name. Immediately report compromised passwords and suspected computer misuse/suspicious activity to an IASO.

6. **Procedures -** Personal Use of Government Computers. There are detailed rules for appropriate and inappropriate use of government computers and the use of government computers for personal tasks. **Government computers are to be used by government employees for official business, authorized personal use, and limited morale and welfare communications between deployed Soldiers and their family members.**

a. Authorized personal use is defined in the DoD Directive 5500.7-R, Joint Ethics Regulation. Authorized personal use includes brief access and searches for information on the internet, sending short email messages, and professional development; additionally, it serves a legitimate public interest, such as furthering the education and self-improvement of employees, improving employee morale and welfare, or job searching in response to downsizing.

b. Personal use of government computers must not overburden the system. Cruising of the Internet for personal or entertainment purposes is not authorized. Additionally, other misuse of government computers includes the following actions and activities: hacking or using hacking tools, visiting hacker web sites, deliberately installing viruses on DoD computers, attempting to bypass security policy and using internet telephony, "streaming" audio/video web sites (e.g., keeping a web page open to receive hourly stock updates), music, and radio stations.

c. The authorized AIS user is personally responsible, under the law, to apply prescribed security policies and procedures contained within this memorandum. This policy is punitive in nature and violators are subject to adverse administrative action and punitive action under the Uniform Code of Military Justice and as otherwise provided by federal law.

7. **Acknowledgement**. Users, supervisors, managers and commanders will acknowledge by signature on the Computer User Agreement that they have read and understood this policy (see enclosure 1). Any questions regarding this policy should be answered by the battalion IASO or Brigade IASO prior to signature. Personnel who refuse to acknowledge this policy will not be granted access to operate a government AIS.

8. All Soldiers, Department of the Army civilians, and contract employees of the 15th Regimental Signal Brigade are expected to fully comply with this policy. Violation of this policy memorandum by any 15th Regimental Signal Brigade Soldier or civilian employee provides a basis for disciplinary action under the Uniform Code of Military Justice or adverse administrative action.

Joseph K Layton

JOSEPH K. LAYTON
COL, SC
Commanding

2 Encls
1. Acceptable User Policy
2. 15th RSB Automation SOP

DISTRIBUTION: B